UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA

MICHAEL YOUNG individually and on behalf of all others similarly situated, **Plaintiff,** **v.** **US RADIOLOGY SPECIALISTS, INC.,** **Defendant.**	**Case No.** **COMPLAINT – CLASS ACITON** Jury Trial Demanded

Plaintiff Michael Young ("Plaintiff"), by and through his attorneys of record, upon personal knowledge as to his own acts and experiences, and upon information and belief as to all other matters, files this complaint against Defendant US Radiology Specialists, Inc. ("US Radiology" or "Defendant") and alleges the following:

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the private and sensitive information it collected, maintained, stored, analyzed, and used to provide its services. This information includes, but is not limited to, personally identifiable information ("PII") and protected health information ("PHI"), including one or more of the following: full name, Social Security number, address, date of birth, health insurance information, medical record number, patient account number, physician name, date(s) of service, diagnosis, and/or treatment information related to radiology services, and driver's license numbers (collectively, "Sensitive Information") hundreds of thousands of patients. [1]

[1] https://www.gatewaydiagnostic.com/privacy-incident/

2. Defendant owns and operates several independent radiology practices located across the country. These clinics include, among others: Gateway Diagnostic Imaging, Radiology Ltd., Charlotte Radiology, Touchstone Medical Imaging, and Diversified Radiology of Colorado. Through its clinics, US Radiology's provides, among other things, primarily diagnostic imaging and related medical services, including X-RAY, CT-SCAN, MRI, and ultrasound to patients located throughout the country. In all, Defendant's clinics are located in at least fourteen states: Alabama, Arizona Arkansas, Colorado, Florida, Georgia, Kansas, Montana, New Jersey, New York, North Carolina, Oklahoma, South Carolina, and Texas.

3. To obtain medical treatment, Plaintiff and other patients entrust and provide an extensive amount of highly sensitive PII to US Radiology, directly, and, indirectly, through the other radiology clinics it owns and operates. US Radiology and its clinics also record an extensive amount of PHI regarding its patients, including diagnoses and treatment information. US Radiology comes to control, store, and maintain its records and the records of its subsidiary clinics even long after the treatment relationship ends.

4. Defendants knew or should have known of the importance of the protected this information. Indeed, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and members of the proposed Class's PII, Defendant assumed legal and equitable duties to those individuals to safeguard that data against the known and well-established risk of a data breach.

5. Plaintiff and members of the proposed Class are victims of Defendant's negligent and/or careless acts and omissions and the failure to protect PII and PHI of Defendant's current and former patients.

6. Specifically, Plaintiff and members of the proposed Class trusted US Radiology and its clinics with their PII and PHI. Defendant betrayed that trust, however, by failing to use

reasonable, up-to-date security practices and protocols to prevent the Data Breach that occurred. Defendant further failed to provide a timely, adequate, and accurate notice to Plaintiff and members of the proposed Class.

7. On information and belief, Defendant began notifying victims about the Data Breach on September 2, 2022–almost 9 months after Defendant became aware of the Breach–Defendant failed to explain why it took so long to notify breach victims. According to Defendant, it first identified the Breach on December 24, 2021.[2]

8. When Defendant finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Defendant's notice sent to impacted individuals fails to explain how many people were impacted, how the breach happened, or why it took so long to send a bare-bones notice to impacted individuals.

9. Plaintiff and members of the proposed Class are victims of Defendant's negligent and/or careless acts and omissions and the failure to protect PII and PHI of Plaintiff and members of the Class.

10. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant did not maintain reasonable, up-to-date security practices and protocols to prevent the Data Breach that occurred. In fact, Defendant confirmed as much in its Breach Notice: "We continue to implement enhancements to information security, systems, and monitoring capabilities."[3]

11. Prior to notification of the breach, Plaintiff and members of the proposed Class had no idea their PII and PHI had been compromised, and that they were, and continue to be, at

[2] Ex. 1.

[3] *Id.*

significant risk of identity theft and various other forms of personal, social, and financial harm. This risk will carry on for the duration of their lifetimes.

12. Defendant's failure to timely detect and notify breach victims violates North Carolina law and has made Plaintiff and members of the Class (defined *infra*) vulnerable to a present and continuing risk of fraud and identity theft.

13. For example, armed with Sensitive Information acquired in the Data Breach, data thieves are able to commit numerous crimes including opening new financial accounts in members of the proposed Class's names, using members of the proposed Class's names to obtain government benefits, filing fraudulent tax returns, obtaining driver's licenses in members of the proposed Class's names but with another person's photograph, giving false information to police during an arrest, taking out loans in members of the proposed Class's names, and using members of the proposed Class's names to obtain medical services. Accordingly, Plaintiff and members of the proposed Class must now and for the foreseeable future closely monitor their financial and other accounts to guard against identity theft and related harm.

14. As a result of Defendant's conduct, Plaintiff and the Class have and will be required to continue to undertake and incur out-of-pocket, expensive, and time-consuming efforts to mitigate the actual and potential impact of the Data Breach on their lives by, among other things, placing freezes and alerts with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, changing passwords on medical portals, and requesting and maintaining accurate medical records outside of those kept by medical providers.

15. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the private and sensitive information it collected, maintained, stored, analyzed, and used in its ordinary course of business.

16. Plaintiff and the members of the proposed Class therefore bring this lawsuit seeking remedies including damages, reimbursement of out-of-pocket-costs, and equitable and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and identity protection services funded by Defendant.

PARTIES

17. **Plaintiff Michael Young** is a resident of Little Elm, Texas where he provided PII and PHI to one of US Radiology's clinics, Gateway Diagnostic Imaging. Mr. Young received a notice dated September 2nd 2022 informing him that his Sensitive Information was compromised during a Data Breach that included Gateway Diagnostic Imaging, which was part of US Radiology's Data Breach.

18. **Defendant U.S. Radiology** operates its headquarters at 4200 Six Forks Road, Suite 100, Raleigh, NC 27609. U.S. Radiology partners with physician-owned radiology practices and diagnostic imaging centers, including Gateway Diagnostics Imaging, and, by doing so, gains control over patients' PII and PHI, including Plaintiff's. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over

cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, Defendant's Data Breach has exposed the data of individuals located in several different states. Therefore, minimal diversity is met because at least one member of the Class is diverse from Defendant.

20. This Court has specific personal jurisdiction over Defendant because it has minimum contacts with this State, as it is located and conducts substantial business here, and Plaintiff's claims arise from Defendant's conduct in this State, due to US Radiology's relationship with Gateway Diagnostic Imaging.

21. This Court is the proper venue for this action pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL BACKGROUND

A. Background

22. US Radiology is a medical company that partners with top private practice radiology groups, outpatient imaging operators, and leading health systems.[4] Sharing best practices, US Radiology claims that by investing in a partnership with US Radiology, radiology groups across the country can elevate patient care.[5]

23. US Radiology advertises that its program ensures that physician partners are "setting the standard in our field: providing top-level, evidence-based care and generating the highest quality outcomes.[6]

[4] https://www.usradiology.com/why-us-radiology

[5] *Id.*

[6] *Id.*

24. US Radiology further advertises that it can help its partners drive productivity and improve processes and patient outcomes through innovative technology and equipment that may not be accessible or affordable for an independent practice or imaging center.[7] US Radiology claims that its investments in areas including "next-generation stack systems, revenue cycle management and database analytics" will help practices streamline operational and financial processes.

25. US Radiology's "Partners" include, among others: Charlotte Radiology, Diversified Radiology, Touchstone Medical Imaging, American Health Imaging, Radiology Ltd., Upstate Carolina Radiology, Windsong Radiology, Gateway Diagnostic Imaging, South Jersey Radiology Associates, and Larchmont Imaging Associates.[8]

26. To obtain healthcare and related services, patients, like Plaintiff and the Class, must provide their PII and PHI to Gateway Diagnostic Imaging and other clinics associated with US Radiology. Upon information and belief, through its Partners, Defendant receives, collects and stores some of Plaintiff's and Class Members' most sensitive and confidential information, including their Social Security numbers, as a condition of rendering medical services. Consequently, US Radiology stores the PII and PHI of hundreds of thousands of individuals per year indicating it has created and maintains a massive repository of Sensitive Information, acting as a particularly lucrative target for data thieves looking to obtain and misuse or sell patient data.

27. Plaintiff and Class Members relied on this sophisticated Defendant to keep their Personal Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their Personal Information.

---

[7] *Id.*

[8] https://www.usradiology.com/partners

28. Defendant, as a healthcare company retaining Personal Information of patients, had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' Personal Information from involuntary disclosure to third parties.

29. Plaintiff and the Class had a reasonable expectation that Defendant would protect the Sensitive Information provided to and created by it, especially because, given the publicity of other data breaches and the significant impact they had, Defendant knew or should have known that failing to adequately protect patient information could cause substantial harm. .

30. As described throughout this Complaint, Defendant did not reasonably protect, secure, or store Plaintiff's and the Class's Sensitive Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Defendant maintained. Consequently, cybercriminals circumvented Defendant's security measures, resulting in a significant data breach.

B. The Data Breach and Notice Letter

31. Beginning on December 17, 2021, to December 24, 2021, a malicious actor gained unauthorized access to Defendant's computer network and systems.[9] By doing so, the actor gained access to the sensitive personal, medical, and insurance information of Defendant's current and former patients. The malicious actors maintained unfettered access to Defendant's network and systems until Defendant remediated the breach and resolved its security vulnerabilities on or around December 24, 2021. Upon information and belief, the actors copied and exfiltrated substantial amounts of Plaintiff's and the Class's PII and PHI.[10]

[9] Ex. 1.

[10] *Id.*

32. The Data Breach appears to have impacted numerous radiology clinics, each associated with US Radiology. Although US Radiology has yet to formally acknowledge to Plaintiff and Class Members that it was the source of a Data Breach affecting hundreds of thousands of individuals, at least eight of its ten Partners have announced identical cybersecurity incidents, pointing towards US Radiology as the entity responsible for releasing Plaintiff's and Class Members' Personal Information.

33. For instance, in February 2022, US Radiology made a report to HHS regarding a cybersecurity incident that compromised Personal Information of 87,552 patients.[8] US Radiology did not provide any additional context as to the details of this cybersecurity incident. Upon information and belief, this is the only acknowledgement of the Data Breach US Radiology has made to date.

34. In the months following US Radiology's report to HHS, Texas's Attorney General's Office received reports from both Gateway Diagnostics and American Health Imaging, two of US Radiology's Partners, notifying the Office of a Data Breach impacting 240,673 Gateway Diagnostics Imaging patients and 21,003 American Health Imaging patients. Gateway Diagnostic Imaging and Radiology Ltd. also submitted breach notices to the Montana Attorney General's office.

35. As of the filing of this complaint, Touchstone Medical Imaging, Charlotte Radiology, Radiology Ltd., Gateway Diagnostics, American Health Imaging, Windsong Radiology[9], Diversified Radiology, and Upstate Carolina Radiology, have all issued public notices of the Data Breach ("Breach Notices"), which Plaintiff believes are connected.

36. The Data Breach notices associated with each of those breaches of radiology clinics are almost word-for-word identical:

> **Notice of IT Security Incident Affecting Certain Patients**
>
> In late 2021, Touchstone Medical Imaging experienced an incident that involved certain patients' information. We have completed our investigation and there is no evidence that this incident resulted in fraud or misuse of the information involved.

> We expect to complete the notification process for all identified individuals by the end of September.
>
> On December 24, 2021, we identified a security incident that impacted systems that contained our patient information. We immediately initiated our incident response process, notified law enforcement, and began an investigation with the assistance of a forensic firm. Within days, we were able to contain the incident and resume serving patients. The investigation subsequently determined that between December 17 and December 24, 2021, an unauthorized party gained access to our network.
>
> Some patients' information may have been accessed, including patient names and one or more of the following: address, date of birth, health insurance information, medical record number, patient account number, physician name, date(s) of service, diagnosis, and/or treatment information related to radiology services. For a limited number of patients, Social Security numbers may have been included. We are offering complimentary credit monitoring to those individuals.
>
> We recommend that patients review the statements they receive from their health insurer. If you see charges for services you did not receive, please call the insurer immediately.
>
> We have also set up a dedicated call center to answer questions about this incident. Patients with questions may call the call center at 1-855-604-1852, Monday through Friday between 8 AM – 8 PM Central Time.
>
> We continue to implement enhancements to information security, systems, and monitoring capabilities and are committed to maintaining the confidentiality and security of patients' information.[11]

37. All eight of the notices of a data breach reference the same timeline for the Data Breach, between December 17 and December 24, 2021, where an unauthorized party gained access to Personal Information. All eight notices also provide the same phone number for a dedicated call center to provide answers to questions regarding the Data Breach and recommend the same course of action for victims to protect themselves.

38. Upon information and belief, the true source of the Data Breach was US Radiology, the common link between the Partners. US Radiology has refused to be transparent with Plaintiff and

[11] *See also* https://www.gatewaydiagnostic.com/privacy-incident/; https://americanhealthimaging.com/wp-content/uploads/2022/09/AHI-Substitute-Notice_9.2.22.pdf

Class Members regarding the circumstances under which their Personal Information was exposed to unauthorized third parties, which is required under both state and federal law.

39. As the notices illustrate, Defendant did not disclose the full scope of the Data Breach to patients or the public until September 2, 2022, over nine months after they initially learned of the Data Breach.

40. The Data Breach notices recommended Plaintiff and the Class take time-consuming steps to mitigate the risk of future fraud and identity theft.

41. Given that Defendant was storing the PII and PHI of Plaintiff and the Class and knew or should have known of the serious risk and harm caused by a data breach, Defendant was obligated to implement reasonable measures to prevent and detect cyber-attacks, such as those recommended by the Federal Trade Commission, required by the Health Insurance Portability and Accountability Act, and promoted by data security experts and other agencies. That obligation stems from the foreseeable risk of a Data Breach given that Defendant collected, stored, and had access to a swath of highly sensitive patient records and data and, additionally, because other highly publicized data breaches at different healthcare institutions put Defendant on notice that the higher personal data it stored might be targeted by cybercriminals.

42. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry and the prevalence of health care data breaches, Defendant inexplicably failed to adopt sufficient data security processes, a fact highlighted in its notification to affected patients in which it revealed that only after the Data Breach, Defendant has taken steps to increase the security of its systems, stating: "We continue to implement enhancements to information security, systems, and monitoring capabilities." Clearly, the Data Breach at issue here was the inevitable result of Defendant's inadequate approach and/or attention to data security

protection of the Sensitive Information it collects, analyzes, and uses in its ordinary course of business.

43. The Data Breach itself, and the information Defendant has disclosed about the breach to date, including its length, the need to remediate Defendant's cybersecurity, the number of people impacted, and the sensitive nature of the impacted data collectively demonstrate Defendant failed to implement reasonable measures to prevent cyber-attacks and the exposure of the Sensitive Information they oversaw.

C. Exposure of Sensitive Information Creates a Substantial Risk of Harm

44. The personal, health, and financial information of Plaintiff and the Class is valuable and has become a highly desirable commodity to data thieves.

45. Defendant's failure to reasonably safeguard Plaintiff's and the Class's sensitive PHI and PII has created a serious risk to Plaintiff and the Class, including both a short-term and long-term risk of identity theft.[12]

46. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[13]

47. This is because stolen Sensitive Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines and is frequented by criminals, fraudsters, and other wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal identities and online activity.

[12] The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority. 17 C.F.R. § 248.201 (2013).

[13] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims,* ThreatPost.com (last visited Jan. 17, 2022), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/

48. Purchasers of Sensitive Information use it to gain access to the victim's bank accounts, social media, credit cards, and tax details. This can result in the discovery and release of additional Sensitive Information from the victim, as well as Sensitive Information from family, friends, and colleagues of the original victim. Victims of identity theft can also suffer emotional distress, blackmail, or other forms of harassment in person or online. Losses encompass financial data and tangible money, along with unreported emotional harms.

49. The FBI's Internet Crime Complaint (IC3) 2019 estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone. The same report identified "rapid reporting" as a tool to help law enforcement stop fraudulent transactions and mitigate losses.

50. Defendant did not rapidly, or even reasonably, report to Plaintiff and the Class that their Sensitive Information had been exposed or stolen.

51. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[14]

52. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require:

(1) encrypting information stored on computer networks;

(2) retaining payment card information only as long as necessary;

[14] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited Jan. 18, 2022) http://www/ftc/gov/speeches/harbour/091207privacyroundtable.pdf.

(3) properly disposing of personal information that is no longer needed or can be disposed pursuant to relevant state and federal laws;

(4) limiting administrative access to business systems;

(5) using industry unapproved activity;

(6) monitoring activity on networks to uncover unapproved activity;

(7) verifying that privacy and security features function property;

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.[15]

53. The United States Government and the United States Cybersecurity & Infrastructure Security Agency recommend several similar and supplemental measures to prevent and detect cyber-attacks, including, but not limited to: implementing an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring firewalls, automating anti-virus and anti-malware programs, managing privileged accounts, configuring access controls, disabling remote desktop protocol, and updating and patching computers.

54. The FTC cautions businesses that failure to protect Sensitive Information and the resulting data breaches can destroy consumers' finances, credit history, and reputations, and can take time, money and patience to resolve the effect.[16] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures—like Defendant failed to do here—as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

D. The Healthcare Industry is Particularly Susceptible to Cyber Attacks.

[15] *Start With Security, A Guide for Business,* FTC (last visited Jan. 18, 2022) https://www.ftc.gov/system/files/documents/plain-language/pdf0205.

[16] *See* Taking Charge, What to Do if Your Identity is Stolen, FTC, at 3 (2012) (last visited Jan. 19, 2022), www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

55. Data breaches have become alarmingly commonplace in the U.S. In 2021, data breaches increased by nearly 70% over the previous year, which is over 20% higher than the previous all-time high.[17]

56. The healthcare sector was the easiest "mark" among all major sectors last year, meaning it had the highest number of data compromises and categorically had some of the most widespread exposure per data breach.[18] According to the 2021 Healthcare Information and Management Systems Society Cybersecurity Survey, 67% of participating hospitals reported having a significant security incident within the last twelve months, with a majority of those being caused by "bad actors."[19]

57. Healthcare providers and vendors that maintain health care provider data "have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.[20]

58. A 2010 report focusing on healthcare data breaches found the "average total cost to resolve an identity theft related incident … came to about $20,000."[21] According to survey results

---

[17] *2021 Annual Data Breach Year-End Review*, ITRC, (Jan. 2022), https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/

[18] *Id.*

[19] *2021 HIMSS Cybersecurity Survey*, Healthcare Information and Management Systems Society, Inc., accessible at: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey (last accessed Mar. 16, 2022).

[20] Benishti, Eyal, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), https://www.idigitalhealth.com/news/how-to-safeguard-hospitaldata-from-email-spoofing-attacks.

[21] *See* Elinor Mills, *Study: Medical identity theft is costly for victims,* CNET (March 3, 2010), (last visited Jan. 11, 2021), https://www.cnet.com/tech/services-and-software/study-medical-identity-theft-is-costly-for-victims/

and population extrapolations from the National Study on Medical Identity Theft report from the Ponemon Institute, nearly 50% of victims reported losing their healthcare coverage because of a data breach and nearly 30% reported an increase in their insurance premiums.[22] Several individuals were unable to fully resolve their identity theft crises. Healthcare data breaches are an epidemic and they are crippling the impacted individuals—millions of victims every year.[23]

59. According to an analysis of data breach incidents reported to the U.S. Department of Health and Human Services and the media, from 2015 and 2019, the number of healthcare related security incidents increased from 450 annual incidents to 572 annual incidents, likely a conservative estimate.[24]

60. According to the Verizon Data Breach Investigations Report, the health care industry, including hospitals and other providers, experienced 655 known data breaches, 472 of which had confirmed data disclosures in 2021.[25] For the tenth year in a row, the healthcare industry has seen the highest impact from cyber-attacks of any industry.[26]

61. As a healthcare provider with numerous medical facilities and hundreds of thousands of current and former patients, if not more, Defendant knew or should have known the

---

[22] *Id.*

[23] *Id.*

[24] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEALTHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=OVer%2041%20million%20patient%20records,close%20to%2021%20million%20records (last visited Jan.19, 2022).

[25] Verizon, 2021 Data Breach Investigations Report: Healthcare NAICS 62 (2021) (last visited Jan. 19, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/healthcare-data-breaches-security/.

[26] *Five worthy reads: The never-ending love story between cyberattacks and healthcare,* ManageEngine, https://blogs.manageengine.com/corporate/manageengine/2021/08/06/the-never-ending-love-story-between-cyberattacks-and-healthcare.html#:~:text=According%20to%20Infosec%20Institute%2C%20credit,is%20%24158%20per%20stolen%20record.

importance of protecting the Sensitive Information entrusted to it. Defendant also knew or should have known of the foreseeable, and catastrophic consequences if its systems were breached. These consequences include substantial costs to Plaintiff and the Class because of the Data Breach. Despite this, Defendant failed to take reasonable data security measures to prevent or mitigate losses from cyberattacks.

E. Plaintiff's and the Class's PHI and PII are Valuable.

62. Unlike financial information, such as credit card and bank account numbers, the PHI and certain PII exfiltrated in the Data Breach cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of her or her life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable to hackers.[27]

63. Birth dates, Social Security numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on an ongoing basis rather than exploiting just one account until it's canceled.[28] For that reason, Cybercriminals on the dark web are able to sell Social Security numbers for large profits. For example, an infant's social security number sells for as much as $300 per number.[29] Those numbers are often then used for fraudulent tax returns.[30]

---

[27] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters, https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited Jan. 18, 2022).

[28] Tim Greene, *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[29] *Id.*

[30] *Id.*

64. Consumers place a considerable value on their Sensitive Information and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth between $30.49 and $44.62.[31] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

65. Defendant's Data Breach exposed a variety of Sensitive Information, including Social Security numbers and PHI.

66. The Social Security Administration ("SSA") warns that a stolen Social Security number can lead to identity theft and fraud: "Identity thieves can use your number and your credit to apply for more credit in your name."[32] If the identity thief applies for credit and does not pay the bill, it will damage victims' credit and cause a series of other related problems.

67. Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

68. PHI, also at issue here, is likely even more valuable than Social Security numbers and just as capable of being misused. The Federal Bureau of Investigation ("FBI") has found

[31] 11-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore,* at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Jan. 19, 2022).

[32] Social Security Administration, *Identity Theft and Your Social Security Number*, (last visited Jan. 19, 2022), https://www.ssa.gov/pubs/EN-05-10064.pdf.

instances of PHI selling for fifty times the price of stolen Social Security numbers or credit card numbers.[33]

69. Other reports found that PHI is ten times more valuable on the black market than credit card information.[34] This is because one's personal health history, including prior illness, surgeries, diagnoses, mental health, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, social security numbers. Credit card information and PII sell for $1-2 on the black market, but PHI can sell for as much as $363 according to the Infosec Institute.[35]

70. Cybercriminals recognize and exploit the value of PHI and PII. The value of PHI and PII is the foundation to the cyberhacker business model.

71. Because the Sensitive Information exposed in the Defendant's Data Breach is permanent data, there may be a gap of time between when it was stolen and when it will be used. The damage may continue for years. Plaintiff and the Class now face years of monitoring their financial and personal records with a high degree of scrutiny. The Class has incurred and will incur this damage in addition to any fraudulent use of their Sensitive Information.

F. Defendant's Conduct Violates HIPAA

72. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), individuals' health information must be:

---

[33] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-healthcare-cyber-intrusions/ (last visited Jan. 18, 2022).

[34] Tim Greene, *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[35] *Hackers Selling Healthcare Data in the Black Market*, INFOSEC, https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 18, 2022).

> properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.[36]

73. HIPAA is a "federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[37] The rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.[38]

74. HIPAA defines sensitive patient personal and health information as: (1) Name; (2) Home and work addresses; (3) Home and work phone numbers; (4) Personal and professional email addresses; (5) Medical records; (6) Prescriptions; (7) Health insurance information; (8) Billing information; (9) Social Security number; (10) Spouse and children's information; and/or (11) Emergency contact information.[39]

75. To ensure protection of this private and sensitive information, HIPAA mandates standards for handling PHI—the very data Defendant failed to protect. The Data Breach resulted from Defendant's failure to comply with several of these standards:

a. Violation of 45 C.F.R. § 164.306(a)(1): failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits;

b. Violation of 45 C.F.R. § 164.312(a)(1): Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;

---

[36] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Jan. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[37] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Jan. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/security/index.html.

[38] *Id.*

[39] *Id.*

c. Violation of 45 C.F.R. § 164.308(a)(1): Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

d. Violation of 45 C.F.R. § 164.308(a)(6)(ii): Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity;

e. Violation of 45 C.F.R. §164.306(a)(2): Failing to protect against any reasonably–anticipated threats or hazards to the security or integrity of electronic protected health information;

f. Violation of 45 C.F.R. §164.306(a)(3): Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information;

g. Violation of 45 C.F.R. §164.306(a)(94): Failing to ensure compliance with HIPAA security standard rules by their workforce;

h. Violation of 45 C.F.R. §164.502, et seq: Impermissibly and improperly using and disclosing protected health information that is, and remains, accessible to unauthorized persons; and

i. Violation of 45 C.F.R. §164.530(c): Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information.

76. Despite Defendant's failure to reasonably protect Plaintiff's and the Class's Sensitive Information, they have not offered any compensation or adequate remedy considering the significant and long-term risks Plaintiff and the Class face.

G. Defendant's *Delay in Identifying and Reporting the Breach Caused Additional Harm*

77. It is axiomatic that:

> The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[40]

[40] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study,* BUSINESS WIRE,

78. Indeed, once a data breach has occurred:

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills, insurance invoices, and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them to catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves (internal citations omitted). [41]

79. As a result of Defendant's delay in detecting and notifying Plaintiff and members of the proposed Class of the Data Breach, Plaintiff and members of the proposed Class's risk of fraud has been driven even higher.

80. Additionally, pursuant to 45 CFR § 164.404, and as outlined in the AFC Joint Privacy Policy, Defendant was required to provide notice to Plaintiff and members of the proposed class no later than 60 days after discovering the breach.

81. Although their Sensitive Information was improperly exposed, viewed, exfiltrated and/or stolen on or about December 17, 2021, affected persons were not notified of the Data Breach by Defendant until, at the earliest, September 2, 2022, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

PLAINTIFF'S EXPERIENCES

82. Plaintiff Michael Young is a resident and citizen of Texas. He is a former patient of Gateway Diagnostic Imaging, an entity associated with US Radiology.

---

https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million (last accessed Mar. 21, 2022).

[41] *The Data Breach Next Door Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too,* CONSUMER REPORTS (January 31, 2019), https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last accessed Mar. 21, 2022).

83. As a condition of receiving healthcare related services, Gateway Diagnostic Imaging required Mr. Young to provide his PII and PHI. Accordingly, Plaintiff Gateway, and indirectly U.S. Radiology with his PII and PHI in order to purchase and receive healthcare services. Upon information and belief, Gateway Diagnostic Imaging provided Plaintiff's PII and PHI to US Radiology or otherwise allowed it to access that data.

84. On or about September of 2022, Plaintiff received notice from Gateway Diagnostic Imaging, which informed him of the Data Breach and that he faced a substantial and significant risk of her PII and PHI being misused. Although Gateway Diagnostic Imaging reported the Data Breach, the real cause was the Data Breach at US Radiology.

85. Plaintiff Marker suffered actual injury from having his sensitive information exposed and/or stolen as a result of the Data Breach including, but not limited to: (a) invasion of privacy; (b) loss of time mitigating the risk of identity theft and fraud; (c) diminution in the value of his Sensitive Information–a form of intangible property that she entrusted to Defendant as a condition of receiving healthcare services; (d) continuous imminent and impending injury arising from the increased risk of financial, medical, and identity fraud and theft; and(e) future cost of credit and identity theft monitoring.

CLASS ALLEGATIONS

86. Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23on behalf of himself and all others similarly situated, as representative of the following Class:

> All persons who received notice or were otherwise sent notice that they were impacted by Defendant's Data Breach.

87. Excluded from the Class are Defendant; its officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest in, is a parent or subsidiary of, or which is otherwise controlled by Defendant; and Defendant's affiliates, legal representatives,

attorneys, heirs, predecessors, successors, and assignees. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

88. Plaintiff reserves the right to modify and/or amend the Class definition, including but not limited to creating additional subclasses, as necessary.

89. All members of the proposed Class are readily identifiable through Defendant's records.

90. **Numerosity.** The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class includes at least 240,673 people. The precise number of Class members is unknown to Plaintiff but may be ascertained from Defendant's records.

91. **Commonality and Predominance.** This action involves common questions of law and fact to the Plaintiff and Class members, which predominate over any questions only affecting individual Class members. These common legal and factual questions include, without limitation:

a. Whether Defendant owed Plaintiff and the other Class members a duty to adequately protect their Sensitive Information;

b. Whether Defendant owed Plaintiff and the other Class members a duty to implement reasonable data security measures due to the foreseeability of a data breach;

c. Whether Defendant owed Plaintiff and the other Class members a duty to implement reasonable data security measures because Defendant accepted, stored, created, and maintained highly sensitive information concerning Plaintiff and the Class;

d. Whether Defendant knew or should have known of the risk of a data breach;

e. Whether Defendant breached its duty to protect the PII and PHI of Plaintiff and other Class members;

f. Whether Defendant knew or should have known about the inadequacies of its data protection, storage, and security;

g. Whether Defendant failed to use reasonable care and reasonable methods to safeguard and protect Plaintiff's and the Class's Sensitive Information from unauthorized theft, release, and disclosure;

h. Whether proper data security measures, policies, procedures and protocols were in enacted within Defendant's offices and computer systems to safeguard and protect Plaintiff's and the Class's Sensitive Information from unauthorized theft, release or disclosure;

i. Whether Defendant's conduct was the proximate cause of Plaintiff's and the Class's injuries;

j. Whether Plaintiff and the Class suffered ascertainable and cognizable injuries as a result of Defendant's misconduct;

k. Whether Plaintiff and the Class are entitled to recover damages; and

l. Whether Plaintiff and the Class are entitled to other appropriate remedies including injunctive relief.

92. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiff on behalf of herself and the Class. Individual questions, if any, are slight by comparison in both quality and quantity to the common questions that control this action.

93. **Typicality.** Plaintiff's claims are typical of those of other Class members because Plaintiff's PHI and PII, like that of every other Class member, was misused and improperly disclosed by Defendant. Defendant's misconduct impacted all Class members in a similar manner.

94. **Adequacy.** Plaintiff will fairly and adequately represent and protect the interest of the members of the Class and has retained counsel experienced in complex consumer class action litigation and intend to prosecute this action vigorously. Plaintiff has no adverse or antagonistic interests to those of the Class.

95. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court.

CLAIMS

COUNT I
Negligence
(On behalf of Plaintiff and the Class)

96. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

97. Defendant collected, created, and maintained Plaintiff's and the Class's Sensitive Information for the purpose of providing medical or related services to Plaintiff and the Class.

98. Plaintiff and the Class are a well-defined, foreseeable, and probable group of patients that Defendant was aware, or should have been aware, could be injured by inadequate data security measures. The nature of Defendant's business requires patients to disclose Sensitive Information to receive adequate care, including, but not limited to, medical histories, dates of birth, addresses, phone numbers, and medical insurance information. Thus, for Defendant to provide its services, it must use, handle, gather, and store the Sensitive Information of Plaintiff and the Class and, additionally, solicit and create records containing Plaintiff's and the Class's Sensitive Information.

99. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. Defendant knew or should have known that, given its repository of a host of Sensitive Information for hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, Defendant had a duty to reasonably safeguard its patients' data by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiff and the Class of inadequate data security created a duty to act reasonably and safeguard the Sensitive Information.

100. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their Sensitive Information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

101. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's and the Class's PHI and PII was adequately protected and secured. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

102. Defendant also had a duty to timely disclose to Plaintiff and the Class that their Sensitive Information had been or was reasonably believed to have been compromised. Timely disclosure is necessary so that, among other things, Plaintiff and the Class may take appropriate measures to monitor their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts and take all other appropriate precautions, including those recommended by Defendant.

103. Additionally, HIPAA creates industry standards for maintaining the privacy of health-related data. Defendant knew or should have known it had a legal obligation to secure and protect Plaintiff's and the Class's Sensitive Information and that failing to do so is a serious violation of HIPAA.

104. Defendant also should have known that, given the Sensitive Information it held, Plaintiff and the Class would be harmed should it suffer a Data Breach. Defendant knew or should have known that its systems and technologies for processing and securing Plaintiff's and the Class's PHI and PII had security vulnerabilities susceptible to cyber-attacks.

105. Despite that knowledge, Defendant failed to implement reasonable data security measures which allowed cybercriminals to successfully breach Defendant's network and data environments, reside there undetected for a significant period of time, and access or steal a host of personal and healthcare information on thousands of Defendant's patients.

106. Defendant, through its actions and/or omissions, failed to provide reasonable security for the data in its possession.

107. Defendant breached its duty to Plaintiff and the Class by failing to adopt, implement, and maintain reasonable security measures to safeguard their Sensitive Information, allowing unauthorized access to Plaintiff's and the Class's PHI and PII, and failing to recognize

the Data Breach in a timely manner. Defendant further failed to comply with industry regulations and exercise reasonable care in safeguarding and protecting Plaintiff's and the Class's PHI and PII.

108. But for Defendant's wrongful and negligent breach of its duties, their Sensitive Information would not have been accessed and exfiltrated by unauthorized persons, and they would not face a risk of harm of identity theft, fraud, or other similar harms.

109. As a result of Defendant's negligence, Plaintiff and the Class suffered damages including, but not limited to, ongoing and imminent threat of identity theft crimes; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Defendant's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; decreased credit scores and ratings; and irrecoverable financial losses due to fraud.

110. As a direct and proximate result of Defendant's negligence, Plaintiff and members of the Class suffered and continue to suffer injuries and are entitled to and demand actual, consequential, and nominal damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
15 U.S.C. § 45
(On behalf of Plaintiff and the Class)

111. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

112. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair ... practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission

("FTC"), the unfair act or practice of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

113. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PHI and PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

114. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

115. Plaintiff and the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

116. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, because of their failure to employ reasonable data security measures, caused the same harm suffered by Plaintiff and the proposed Class.

117. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members suffered and continue to suffer injuries as described herein and are entitled to damages in an amount to be proven at trial.

COUNT III
Negligence *Per Se*
HIPAA, 45 C.F.R. § 160.102
(On behalf of Plaintiff and the Class)

118. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

119. Defendant required Plaintiff and the Class to provide nonpublic Sensitive Information to obtain medical services. During the provision of those services, Defendant created and stored even more PHI.

120. As a healthcare provider, Defendant is covered by HIPAA, 45 C.F.R. § 160.102, and is therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

121. HIPAA, 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information."

122. Per 45 C.F.R. § 164.306, HIPAA "standards, requirements and implementation specifications" apply to covered entities, such as Defendant. HIPAA standards are mandatory.

123. HIPAA requires Defendant to "ensure the confidentiality, integrity, and availability of all electronic protected health information" it receives and to protect against any "reasonably anticipated threats or hazards to the security or integrity" of the Sensitive Information. 45 C.F.R. § 164.306.

124. Defendant violated HIPAA by failing to adhere to and meet the requirements of 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

125. Additionally, HIPAA requires timely notice of data breaches to each impacted consumer and defines timely as "in no case later than 60 calendar days after discovery of the breach." 45 C.F.R. § 164.404. The notice must include certain minimum information, including, but not limited to a description of what the entity is doing to investigate the breach and mitigate harm. *Id.*

126. Defendant breached its HIPAA's notification duty by failing to give timely and complete notice. Defendant waited approximately nine months from the date it was made aware

of the Data Breach to begin contacting victims and the notice did not include any explanation of what the company was doing to mitigate harm.

127. Defendant violated HIPAA by failing to use reasonable measures to protect the PII and PHI of Plaintiff and Class. Defendant's conduct was especially unreasonable given the nature of the Sensitive Information and the number of patients it serves, some of which are minors or patients who live below the federal poverty level, who may not have the means to expend significant amounts of time and money to fully mitigate the fallout of the Data Breach.

128. Defendant's violation of HIPAA constitutes negligence *per se*. Plaintiff and the Class are within the group of individuals HIPAA was designed to protect and the harm to these individuals is a result of the Data Breach.

129. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members suffered and continue to suffer injuries as described herein and are entitled to damages in an amount to be proven at trial.

COUNT IV
VIOLATION OF NORTH CAROLINA'S UNFAIR AND DECEPTIVE TRADE PRACTICES ACT
N.C. Gen. Stat. § 75-1.1, *et seq*.
(on behalf of Plaintiff and the Class)

130. The North Carolina Unfair and Deceptive Trade Practices Act ("NCUDTPA") prohibits "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" N.C. Gen. Stat. § 75-1.1(a).

131. Under the act, "commerce" includes "all business activities, however, denominated[.]" *Id.* at § 75-1.1(b).

132. Furthermore, "any person . . . injured . . . by reason of any act or thing done by any other person, firm or corporation in violation of this Chapter, such person . . . so injured shall have a right of action on account of such injure done[.]" *Id.* at § 75-16.

133. Defendant's conduct was unfair and deceptive in violation of the NCUDTPA. Specifically, Defendant represented that it could adequately protect health care clinics' patient information and that its platforms were safe and secure. It solicited business through these representations and, in turn, gained access to and control over Plaintiff's and the Class's data, even without their knowledge.

134. Defendant, however, could not adequately protect patient data, and designed an insecure platform lacking reasonable data security measures and entirely inadequate to protect the highly sensitive data it collected and stored. Defendant knew or should have known that its data security was inadequate and put Plaintiff and the Class at risk.

135. Additionally, under N.C. Gen. Stat. §§ 75-61, 75-65, businesses impacted by a data breach must provide notice without reasonable delay. Defendant, however, waited almost three months to notify the clinics of the scope and extent of the Data Breach. Because Defendant required the clinics to notify the impacted patients rather than notifying them on its own, Defendant caused further delays to in the notice to customers.

136. Defendant's conduct was, thus, unethical, unscrupulous, substantially injurious to patients, and against North Carolina's stated policy of quickly providing notice of a data breach.

137. Defendant's conduct was also in and affecting commerce because it concerned the provision of services at healthcare clinics. Specifically, Defendant provided software to its clients, the healthcare clinics, which in turn assisted the clinics in providing healthcare related services, and in particular, ophthalmology and optometry services to patients.

138. As a direct and proximate result of Defendant's violation of this Act, Plaintiff and Class members suffered and continue to suffer injuries and are entitled to damages in an amount to be proven at trial.

139. Consequently, Plaintiff seeks actual and compensatory damages, injunctive relief, attorneys' fees and expenses, and all other remedies available under law and awarded by the Court.

COUNT V
Declaratory Judgment
(On behalf of Plaintiff and the Class)

140. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

141. Pursuant to the Uniform Declaratory Judgment Act, §37.003, Courts of record within their respective jurisdiction have the power to declare rights, status, and other legal relations, whether or not further relief is or could be claimed. Further, this Court has the power to declare either affirmative or negative decrees in form and effect, such as restraining acts that violate the laws described in this Complaint.

142. Whether Defendant's actions caused the Data Breach and its subsequent harm to Plaintiff and the Class, and whether Defendant is presently maintaining adequate data security measure to safeguard Plaintiff and the Class from further data breaches is an actual controversy.

143. Plaintiff and the Class are at a substantial and imminent risk of further compromise of their Sensitive Information. This is true irrespective of whether Plaintiff and the Class are current patients of Defendant because Defendant still maintains a swath of Plaintiff's and the Class's Sensitive Information.

144. Pursuant to its authority under the Uniform Declaratory Judgment Act, this Court should enter a judgment declaring the following:

a. Defendant owed a legal duty, at the time of the Data Breach, to Plaintiff and members of the proposed Class to reasonably protect and secure their Sensitive Information under the common law, HIPAA, FTC Act, 15 U.S.C. § 45(a)(1), and FCRA, 15 U.S.C. § 1681(b);

b. Defendant owed a legal duty to Plaintiff and members of the proposed Class to provide timely notice of the Data Breach under the common law, HIPAA, FTC Act, 15 U.S.C. § 45(a)(1), and FCRA, 15 U.S.C. § 1681(b);

c. Defendant continues to owe a legal duty to Plaintiff and members of the proposed Class to protect and secure their Sensitive Information under the common law, HIPAA, FTC Act, 15 U.S.C. § 45(a)(1), and FCRA, 15 U.S.C. § 1681(b);

d. Defendant continues to owe a legal duty to Plaintiff and members of the proposed Class to provide timely notice of data breaches under the common law, HIPAA, FTC Act, 15 U.S.C. § 45(a)(1), and FCRA, 15 U.S.C. § 1681(b);

145. Defendant continues to breach its legal duties by failing to employ reasonable measures to protect and secure Plaintiff's and the putative Class members' Sensitive Information, including that of new patients who are without notice of the Data Breach.

PRAYER FOR RELIEF

146. WHEREFORE, Plaintiff respectfully prays for judgment in her favor as follows:

a. Certification of the Class pursuant to Fed. R. Civ. P. 23 and an order that notice be provided to all Class Members;

b. Designation of Plaintiff as representative of the Class and the undersigned counsel, as Class Counsel;

c. An award of damages in an amount to be determined at trial or by this Court;

d. An order for injunctive relief, enjoining Defendant from engaging in the wrongful and unlawful acts described herein;

e. An award of statutory interest and penalties;

f. Pre-judgment interest at the maximum amount allowed by law;

g. Post-judgment interest at the maximum rate allowed by law;

h. An award of costs and attorneys' fees; and

i. Such other relief the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

147. Plaintiff hereby demands a trial by jury of all issues so triable.

Respectfully submitted,

s/ Jean S. Martin
Jean S. Martin (NC Bar No. 25703)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin St., 7th Floor
Tampa, FL 33602
(813) 559-4908
jeanmartin@forthepeople.com

Joseph M. Lyon*
THE LYON FIRM
2754 Erie Ave.
Cincinnati, Ohio 45208
Telephone: (513) 381-2333
jlyon@thelyonfirm.com

Brian C. Gudmundson*
ZIMMERMAN REED LLP
1100 IDS Center

80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
brian.gudmundson@zimmreed.com

Terence R. Coates*
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Pro Hac Vice Forthcoming